(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07200617 A**

(43) Date of publication of application: **04.08.95**

(51) Int. Cl **G06F 17/30**

(21) Application number: **06000837**

(22) Date of filing: **10.01.94**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

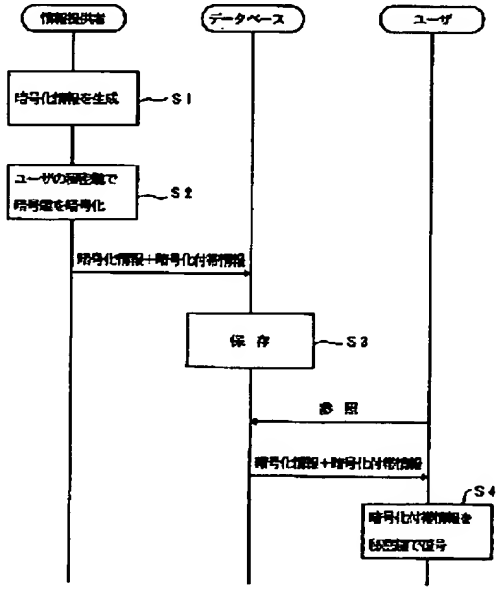
(72) Inventor: **OTA YUKIYOSHI**
SHIMIZU AKIHIRO

(54) CONTROL METHOD FOR REFERENCE RIGHT OF SHARED INFORMATION

(57) Abstract:

PURPOSE: To set a user free from managing many secret keys when all user groups having the same reference right for each information are set by securing the correspondence between the user groups and the coding incidental information obtained by coding the coding key of the information by the secret key of the user.

CONSTITUTION: An information provider codes the offering information by a certain coding key and generates the coding information (S1). Then the coding key is coded by means of a secret key that is shared by the information provider and a user who has the reference right to the offered information (S2). The secret key is stored in a data base together with the coding information as the coding incidental information (S3). In a reference mode, a user of a user group having the reference right acquires the coding information and the coding incidental information from the data base. Then the user decodes the coding incidental information by the secret key in order to calculate a coding key (S4) and then decodes the coding information by the coding key to obtain the offered information. Therefore the user has not to manage many secret keys.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－200617

(43)公開日　平成７年(1995)８月４日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　17/30				
		9194－5L	Ｇ０６Ｆ　15/ 40	３２０　Ｂ

審査請求　未請求　請求項の数２　ＯＬ　（全 9 頁）

(21)出願番号　特願平6－837

(22)出願日　平成６年(1994)１月10日

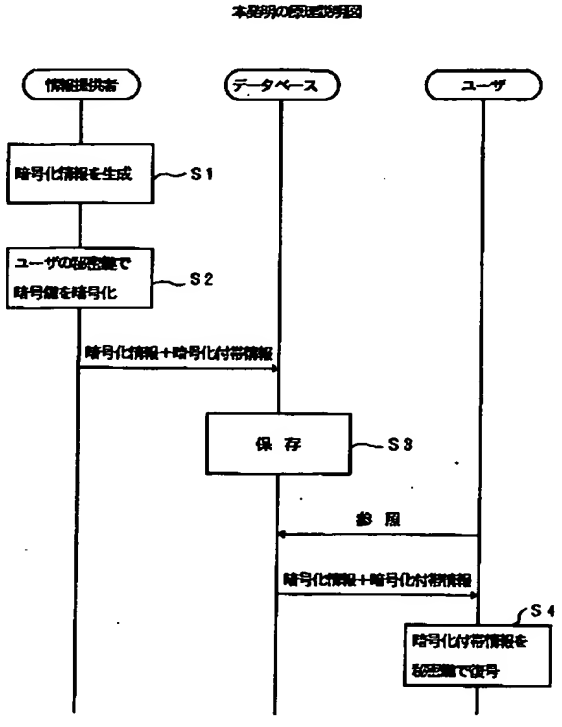
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　大田　幸由
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　清水　明宏
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】　共有情報参照権限制御方法

(57)【要約】

【目的】　本発明の目的は、共有される暗号化情報を参照時に、情報毎に参照権限を同一とするユーザグループを全て設定する場合において、ユーザが多数の秘密鍵を管理しなくともよい共有情報参照権限制御方法を提供することである。

【構成】　本発明は、参照権限のあるユーザで共有されている秘密鍵で暗号化し、　暗号化情報と共に暗号化付帯情報としてデータベースの登録し、暗号化付帯情報を秘密鍵で復号し、復号した暗号化鍵で暗号化情報を復号する。



1

【特許請求の範囲】

【請求項１】　データベースを利用して複数のユーザグループ間で情報の共有を行う方法において、

情報提供者が提供情報をある暗号化鍵で暗号化して暗号化情報を生成し、

該暗号鍵を予め該情報提供者と該提供情報への参照権限のあるユーザで共有されている秘密鍵で暗号化し、

前記暗号化情報とともに、該秘密鍵を暗号化付帯情報としてデータベースに保存し、

参照時には、参照権限のあるユーザグループのユーザが、該データベースから得られる該暗号化情報及び該暗号化付帯情報のうち、該暗号化付帯情報を該秘密鍵を用いて復号することにより暗号化鍵を算出し、

該暗号化鍵で該暗号化情報を復号することにより該提供情報を入手することを特徴とする共有情報暗証権限制御方法。

【請求項２】　前記ユーザをＮ個の要素に対応させて分類し、前記暗号化付帯情報として前記暗号化鍵をＮ分割し、分割された該分割暗号化鍵をそれぞれの該要素に対応する秘密鍵で暗号化したものを合わせて暗号化付帯情報とし、

該暗号化付帯情報を該秘密鍵で復号することにより得られるＮ個の分割暗号化鍵を組み合わせて元の暗号化鍵を得る請求項１記載の共有情報参照権限制御方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、共有情報参照権限制御方法に係り、特に、分散して管理されている情報を、ネットワークを利用して共有するシステムにおいて、暗号方式を利用して、ユーザの権限に応じて情報への参照権限を制御する共有情報参照権限制御方法に関する。

【０００２】

【従来の技術】図８は、共有システムの概要を示す。共有システムは、ネットワークを介して、情報提供者１００がデータベース２００に情報を登録し、ユーザ３００がその情報を参照するシステムである。

【０００３】図８に示す情報共有システムに暗号化技術を適用する基本的な方法として、情報を暗号化してデータベース２００へ登録し、情報の参照権限があるユーザに対してのみ暗号化鍵を配布する方式がある。この方式を図９に示す。

【０００４】暗号化には、ＦＥＡＬ（高速データ暗号化アルゴリズム），ＤＥＳ（データ暗号化規格）などの共通鍵アルゴリズムが用いられる。

【０００５】この方式は、登録段階で情報を暗号化しているため、ネットワーク及びデータベース上で情報の秘密を保持できる。ユーザの権限に応じた参照権限の制御を行うためには、情報（Ｐａ，Ｐｂ，…，Ｐｚ）毎に、ユーザ毎の秘密鍵で暗号化するか、或いは、参照権限を同一とするユーザグループに対応する秘密鍵（Ｋａ，Ｋｂ，…，Ｋｚ）で暗号化する。

2

【０００６】例えば、情報Ｐａをユーザが有する暗号化鍵Ｋａで暗号化して、データベース２００内に暗号化情報ＥＫａ(Ｐａ)として登録しておく。ユーザＡは秘密鍵Ｋａを有し、登録されている暗号化情報ＥＫａ(Ｐａ)を参照をする場合には、秘密鍵（暗号化鍵）Ｋａにより当該暗号化情報ＥＫａ(Ｐａ)を復号し、情報Ｐａを得る。

【０００７】

【発明が解決しようとする課題】しかしながら、ユーザ毎の秘密鍵で暗号化した場合には、ユーザ毎に暗号化情報を用意しなければならないので、非常に冗長である。また、ユーザグループに対応する秘密鍵で暗号化した場合には、以下のような問題がある。

【０００８】ユーザグループの構成が変化したとき、関連するメンバの秘密鍵を変更しなければならい。或いは、予めすべてのユーザグループの秘密鍵を用意するとすれば、情報提供はユーザの所属するユーザグループに対応する複数の秘密鍵をユーザに配送しなければならないと共に、ユーザは所属するユーザグループに対応する複数の秘密鍵を管理しなければならない。

【０００９】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、情報毎に参照権限を同一とするユーザグループを全て設定する時に、ユーザが多数の秘密鍵を管理しなくともよい共有情報参照権限制御方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】図１は、本発明の原理説明図である。

【００１１】本発明は、データベースを利用して複数のユーザグループ間で情報の共有を行う方法において、情報提供者が提供情報をある暗号化鍵で暗号化して暗号化情報を生成し（ステップ１）、暗号鍵を予め情報提供者と提供情報への参照権限のあるユーザで共有されている秘密鍵で暗号化し（ステップ２）、暗号化情報とともに、秘密鍵を暗号化付帯情報としてデータベースに保存し（ステップ３）、参照時には、参照権限のあるユーザグループのユーザが、データベースから得られる暗号化情報及び暗号化付帯情報のうち、暗号化付帯情報を秘密鍵を用いて復号することにより暗号化鍵を算出し（ステップ４）、暗号化鍵で暗号化情報を復号することにより提供情報を入手する。

【００１２】また、本発明は、ユーザをＮ個の要素に対応させて分類し、暗号化付帯情報として暗号化鍵をＮ分割し、分割された分割暗号化鍵をそれぞれの要素に対応する秘密鍵で暗号化したものを合わせて暗号化付帯情報とし、暗号化付帯情報を秘密鍵で復号することにより、得られるＮ個の分割暗号化鍵を組み合わせて元の暗号化鍵を得る。

【００１３】

【作用】本発明は、情報提供者が情報をある暗号化鍵で

暗号化して暗号化情報とし、さらにその暗号化鍵を予め情報提供者と情報への参照権限のあるユーザで共有されている秘密鍵で暗号化し、暗号化情報と共に秘密鍵で暗号化された暗号鍵を暗号化付帯情報としてデータベースに保存しておく。参照権限のあるユーザがデータベースに保存されている暗号化情報を参照する場合には、データベースから得られる暗号化情報及び暗号化付帯情報のうち、暗号化付帯情報を情報提供者と共有される秘密鍵を用いて復号することにより暗号化鍵を求め、この暗号化鍵で暗号化情報を復号することにより、復号化情報を入手する。これにより、情報の暗号化鍵をユーザの秘密鍵で暗号化した暗号化付帯情報をユーザグループに対応させることにより、ユーザの秘密鍵をユーザグループ毎に変更する必要がない。従って、参照権限を同一とするユーザグループを全て設定する時に、多数の秘密鍵を管理しないで済む。

【００１４】また、Ｎ個の要素に分類されたユーザが当該要素に対応する暗号鍵を設定することにより、ユーザは分離された要素の秘密鍵のみを管理することにより暗号化付帯情報量が低減される。

【００１５】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【００１６】《第１の実施例》図２は、本発明の第１の実施例の共有情報を参照する場合のシステム構成を示す。同図に示す例は、情報提供者１００が情報をデータベース２００に登録し、登録されている情報をユーザ３００が参照する場合である。

【００１７】情報提供者１００は、暗号化鍵（Ｋ）をユーザ３００の個別な秘密鍵（Ｋ１，Ｋ２，…，Ｋｎ）で暗号化して得られる暗号化付帯情報２２０（ＥＫ１（Ｋ），ＥＫ２２（Ｋ），…，ＥＫｎ（Ｋ））を暗号化情報２１０とともにデータベース２００に登録する。ユーザ３００は、データベース２００から暗号化情報２１０と暗号化付帯情報２２０を参照する。ユーザ３００がデータベース２００の暗号化情報２１０及び暗号化付帯情報２２０を参照する場合には、まず、暗号化付帯情報２２０を自分の秘密鍵Ｋｎによって復号し、暗号化鍵Ｋを得る。この暗号化鍵Ｋを用いてユーザ３００は、暗号化情報２１０を復号することができる。

【００１８】具体的には、情報提供者１００が情報Ｐをデータベース２００に登録する場合には、
暗号化鍵Ｋを用いて情報Ｐを暗号化し、暗号化情報ＥＫ(P)としてデータベース２００に登録する。
さらに、情報提供者１００は、ユーザ３００_1と共有する秘密鍵Ｋ１を用いて、暗号化鍵Ｋを暗号化し、暗号化付帯情報２２０として、データベース２００に登録する。
次にユーザ３００_1がデータベース２００に登録されている暗号化情報２１０ＥＫ(P)を参照する場合には、データベース２００より暗号化付帯情報２２０を参照し、自分が有する秘密鍵Ｋ１で暗号化付帯情報２２０を復号し、暗号化鍵Ｋを得る。
ユーザ３００_1は、得られた暗号化鍵Ｋを用いてデータベース２００より検索した暗号化情報２１０ＥＫ(P)を復号して、情報提供者１００から提供された情報Ｐを得る。

【００１９】このような方法をとることにより、ユーザ３００は暗号化付帯情報２２０より暗号化情報２１０の暗号化鍵をユーザ個別の秘密鍵を用いて情報を得ることができる。

【００２０】《第２の実施例》上記の第１の実施例より明らかなように、ユーザは個別な秘密鍵Ｋｎだけを管理すればよいが、暗号化情報は、情報提供者が送る情報に比して容量が小さいので本実施例の冗長度は従来と比較して低くなる。これは、暗号化情報２１０毎に管理されている暗号化付帯情報２２０がユーザ数に比例して線形的に増加するためである。本実施例では、ユーザ数が多い時に、暗号化付帯情報量を低減しかつ、冗長度を高めるための方法を以下に示す。

【００２１】図５は、本発明の第２の実施例を説明するための図である。本実施例では、ユーザグループを組織の階層とグループを対応させて分類する。

【００２２】ユーザ全体を組織として、この組織内でユーザを階層、グループという２つの属性によって規定する。

【００２３】各ユーザは、所属グループ間で共通な秘密鍵と所属階層間で共通な秘密鍵の一意の組み合わせを持ち、また、情報提供者１００は、ある２（Ｎ）個の分割暗号化鍵に対して、その排他的論理和をとると暗号化鍵になるように設定する。

【００２４】情報提供者１００が情報の参照権限を組織の階層構造に対応するユーザグループに設定する場合に、情報をある暗号化鍵で暗号化して暗号化情報２１０とし、そのユーザグループに含まれるユーザに対して、２つの分割暗号化鍵の一方を各ユーザの所属グループ用の秘密鍵とし、もう一方を所属階層用の秘密鍵で暗号化して得られる情報を、暗号化付帯情報２２０として暗号化情報２１０と共にデータベース２００に登録する。参照権限のあるユーザ３００は、所持するグループ用の秘密鍵と階層用の秘密鍵を用いて２つの分割暗号化鍵を復号し、これらの排他的論理和等をとることにより暗号化鍵を得る。ユーザ３００はこの暗号化鍵を用いて情報を入手することができる。

【００２５】処理の手順を情報提供者１００、ユーザ３００、及び暗号情報を蓄積するデータベース２００に分けて説明する。階層がＬ１，Ｌ２の２つ、また、グループがＧａ，Ｇｂ，Ｇｃの３つからなる組織における処理の例を用いて示す。

【００２６】［情報提供者］

5

・秘密鍵の管理は、図５に示すように、全ての階層、グループに対して秘密鍵を決定し管理する。同図の例では、例えば、階層“Ｌ１”の秘密鍵として“Ｋ１”を管理し、グループ“Ｇａ”の秘密鍵として“Ｋａ”を管理する。

【００２７】・情報の登録は、あるユーザグループに対応する情報（Ｐ）を登録する際には、２つの分割暗号化鍵（Ｘ，Ｙ）の排他的論理和で得られる暗号化鍵（Ｋ）を用いて情報を暗号化する。登録する暗号化情報２１０（ＥＫ（Ｐ））には、そのユーザグループに含まれる階層の秘密鍵（Ｋ１）を用いて階層名（Ｌ１）及び分割暗号化鍵（Ｘ）を暗号化した情報（ＥＫ１（Ｌ１）ＥＬ１（Ｘ））とそのユーザグループに含まれるグループの秘密鍵（Ｋａ／Ｋｂ）を用いてグループ名（Ｇａ／Ｇｂ）及びもう一方の分割暗号化鍵（Ｙ）を暗号化した暗号化付帯情報２２０（ＥＫａ（Ｇａ），ＥＫａ（Ｙ）／ＥＫｂ（Ｇｂ），ＥＫｂ（Ｙ））を付加しておく。

【００２８】［ユーザ（階層：Ｌ１，グループ：Ｇａ）］

・図５は本発明の第２の実施例のユーザが管理する秘密鍵の情報を示す。同図の例では、自分が所属する階層の秘密鍵（Ｋ１）、グループの秘密鍵（Ｋａ）を管理する。

【００２９】図６は、本発明の第２の実施例のユーザが情報の参照を行う場合の処理を説明するための図である。

【００３０】・情報の参照は、階層Ｌ１，グループＧａに属するユーザがデータベース２００より検索した場合、ユーザ暗号化情報に付加されている暗号化付帯情報２２０

『ＥＫ１（Ｌ１）：ＥＫ１（Ｘ）』

『ＥＫａ（Ｇａ）：ＥＫａ（Ｙ）』

『ＥＫｂ（Ｇｂ）：ＥＫｂ（Ｙ）』

が渡される。このうち、当該ユーザが保持している秘密鍵（Ｋ１），（Ｋａ）で復号した結果、自分が所属する階層（Ｌ１）が得られれば、その時得られる分割暗号化鍵（Ｘ）３１０を保持する。さらに、自分が所持しているグループの秘密鍵（Ｋａ）で復号し、自分が所属するグループ（Ｌａ）が得られれば、その時得られる分割暗号化鍵（Ｙ）３２０と先に階層の秘密鍵（Ｋａ）によって得られた分割暗号化鍵（Ｘ）との排他的論理和で得られる暗号化鍵（Ｋ）３３０を用いて暗号化情報（ＥＫ（Ｐ））３４０を復号する。これにより、情報提供者１００からの情報Ｐが得られる。

【００３１】・情報の登録は、情報提供者として自分を含むユーザグループ内で共有したい暗号化情報２１０をデータベース２００に登録する際には、どのユーザグループに対する情報の登録であるかの情報を用いてそのユーザグループに対応する暗号化付帯情報２２０の作成を行い、暗号化付帯情報２２０に基づいて登録すべき情報

6

を暗号化し暗号化情報２１０とし、暗号化付帯情報２２０と共にデータベース２００に登録する。

【００３２】［データベース］図７は、本発明の第２の実施例のデータベースの登録情報を示す。同図は、階層Ｌ１，グループＧａ，Ｇａのユーザグループに対する登録情報である。データベース２００が情報を管理する場合には、暗号化情報２１０を暗号化する際に用いられた暗号化付帯情報２２０を暗号化情報２１０に付加して管理する。データベース２００の登録される情報は、図７に示すような構造になっているため、ユーザは、暗号化情報２１０の暗号化鍵Ｋを階層の秘密鍵Ｋ１とグループの秘密鍵Ｋａ，Ｋｂを用いて、暗号化付帯情報２２０から得ることができる。また、同一階層に属するユーザは、共通な階層の秘密鍵（Ｋ１）を有し、同一グループに属するユーザは共通なグループの秘密鍵（Ｋａ又は、Ｋｂ）を有するために、この秘密鍵で分割暗号化鍵を暗号化した情報（Ｐ）は、ユーザ間で共通なものとなる。従って、階層とグループの組み合わせ数のユーザを含むユーザグループに対応する暗号化付帯情報２２０を生成しても情報量は、階層とグループの総数に比例したものとなる。

【００３３】この結果から明らかなように、ユーザは、階層の秘密鍵、グループの秘密鍵だけを管理すればよい。また、前述の第１の実施例に比べて暗号化付帯情報量を低減することが可能となる。

【００３４】なお、本発明は、上記の実施例に限定されるものではなく、上記実施例では、ユーザが階層とグループという２種類の要素で分類したが、この例に限定されることなく、期間、場所等の他の要素に置き換える、また、他の要素を付加してもよい。

【００３５】さらに、ユーザを分類する要素を上記では、階層とグループの２種類に分類したが、この例に限定されることなく、ユーザをＮ個の要素で分類してもよい。この場合には、ユーザはＮ個の秘密鍵を有し、これらの秘密鍵を用いて分割暗号化鍵を得る。その後の処理は、上記実施例と同様に当該分割暗号化鍵を用いて復号することにより、情報提供者から提供された情報を得る。

【００３６】

【発明の効果】上述のように本発明によれば、情報の暗号化鍵をユーザの秘密鍵で暗号化した暗号化付帯情報をユーザグループに対応させている。従って、ユーザの秘密鍵をユーザグループ毎に変更する必要ないために、参照権限を同一とするユーザグループを全て設定する時に、多数の秘密鍵を管理しなくともよい。

【図面の簡単な説明】

【図１】本発明の原理説明図である。

【図２】本発明の第１の実施例の共有情報を参照する場合のシステム構成図である。

【図３】本発明の第２の実施例を説明するための図であ

る。

【図４】本発明の第３の実施例の情報提供者が管理する秘密鍵を示す図である。

【図５】本発明の第２の実施例のユーザが管理する情報を示す図である。

【図６】本発明の第２の実施例のユーザが情報の参照を行う場合の処理を説明するための　図である。

【図７】本発明の第２の実施例のデータベースの登録情報を示す図である。

【図８】共有システムの概要を示す図である。

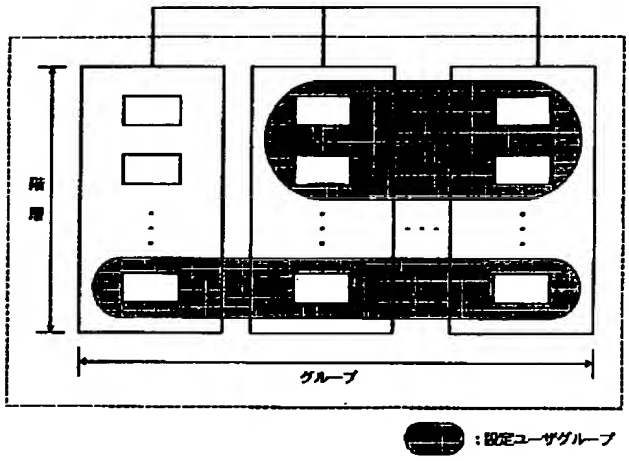
【図９】情報共有システムに暗号化技術を適用した例を＊示す図である。

【符号の説明】

１００　情報提供者
２００　データベース
２１０　暗号化情報
２２０　暗号化付帯情報
３００　ユーザ
３１０　分割暗号化鍵
３２０　分割暗号化鍵
３３０　排他的論理和で得られる暗号化鍵
３４０　暗号化情報

【図３】

本発明の第２の実施例を説明するための図



【図４】

本発明の第３の実施例の情報提供者が管理する秘密鍵を示す図

情報提供者

階層，グループ	鍵
L１	K１
L２	K２
Ga	Ka
Gb	Kb
Gc	Kc

【図５】

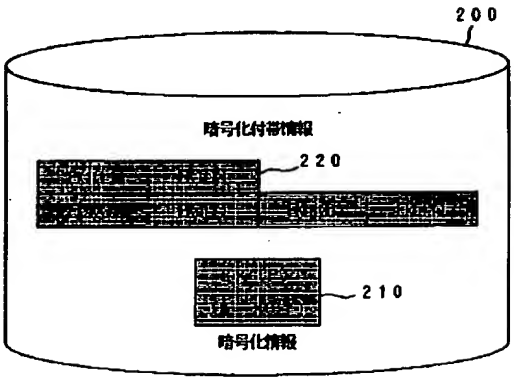
本発明の第２の実施例のユーザが管理する情報を示す図

ユーザ（階層：Ｌ１，グループ：Ga）

階層，グループ	鍵
L１	K１
Ga	Ka

【図７】

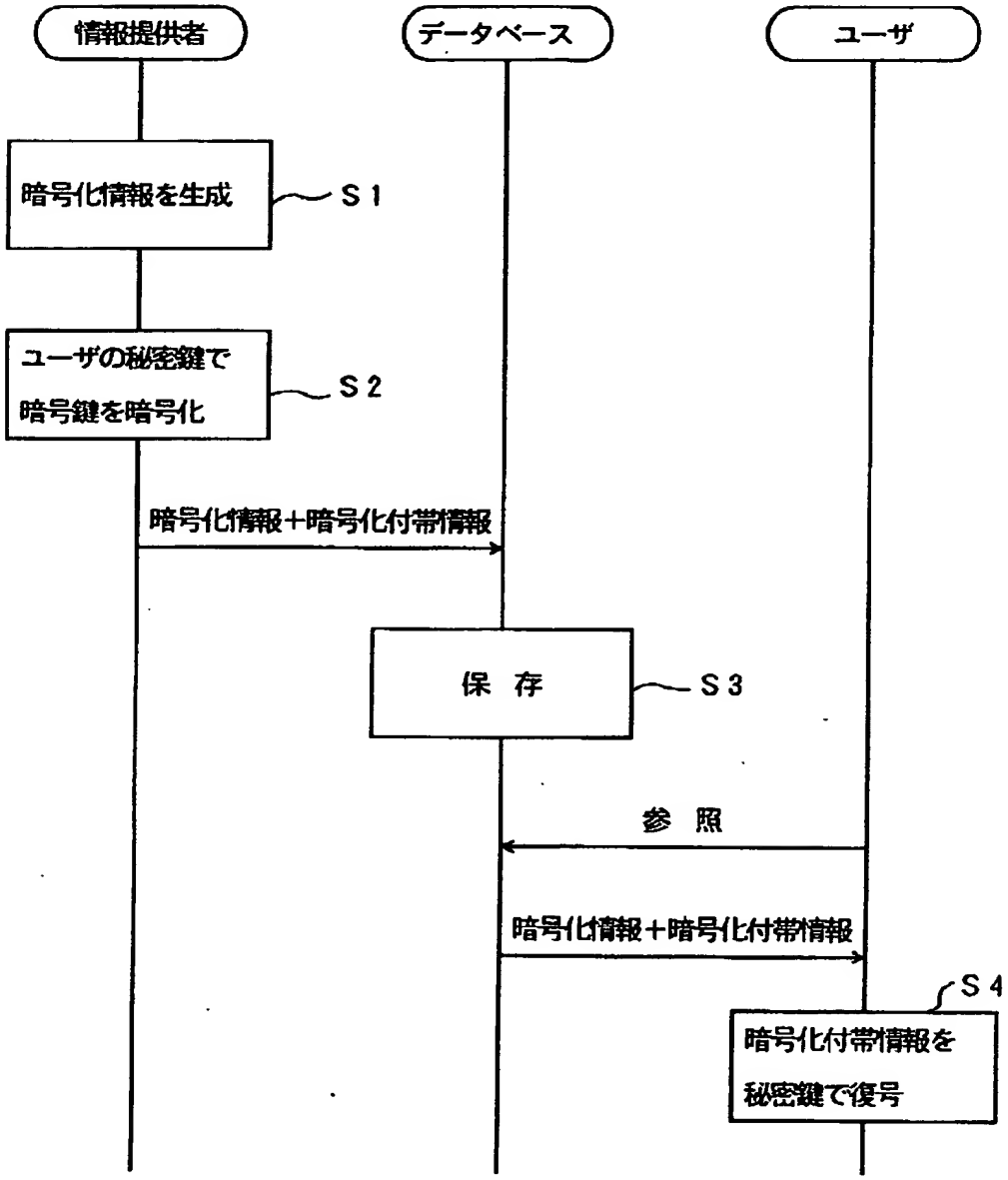
本発明の第２の実施例のデータベースの登録情報を示す図



階層Ｌ１，グループGa，Gbのユーザグループに対する登録情報

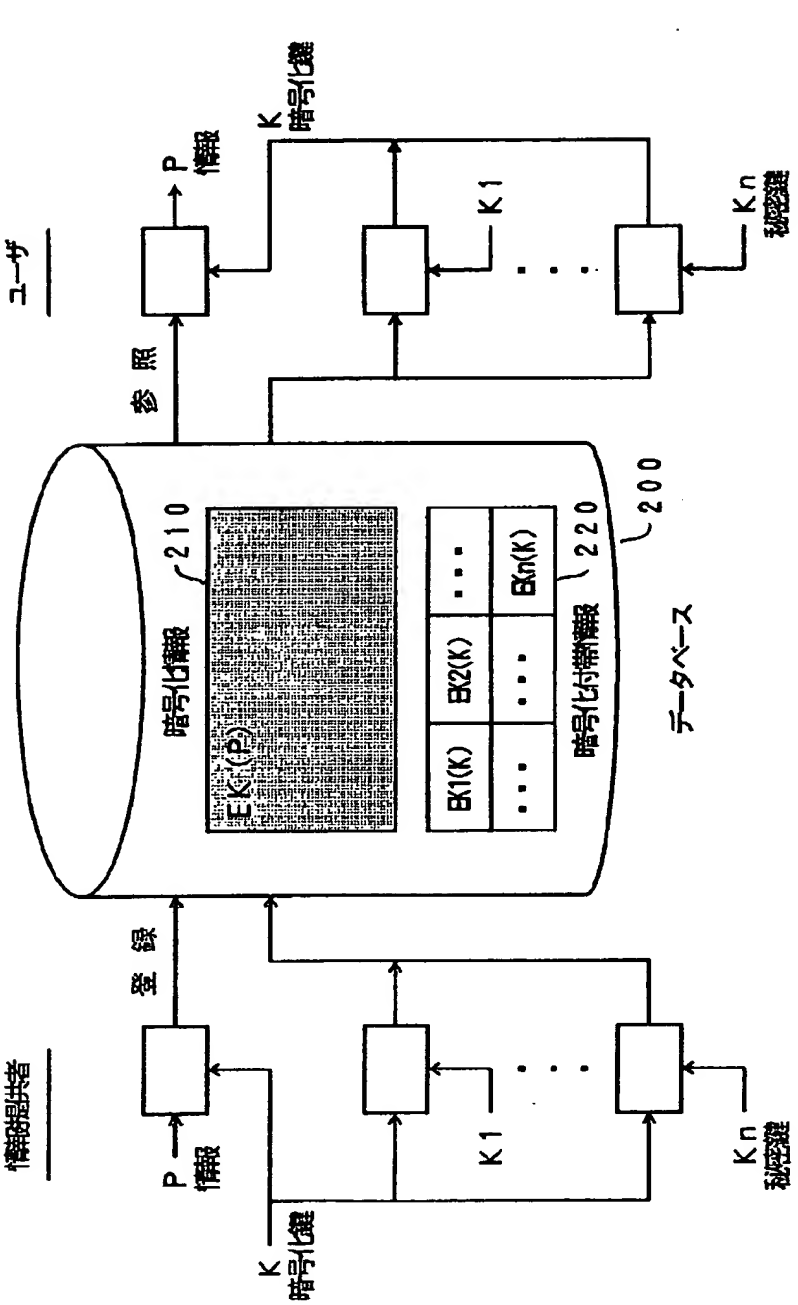
【図１】

本発明の原理説明図



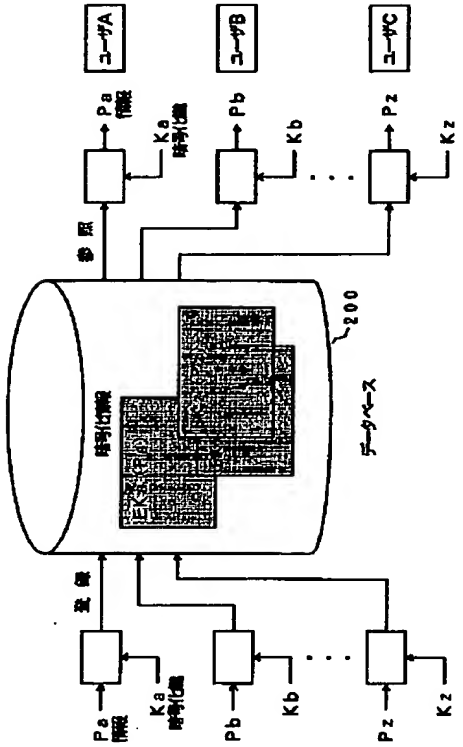
【図２】

本発明の第１の実施例の共有情報を
参照する場合のシステム構成図



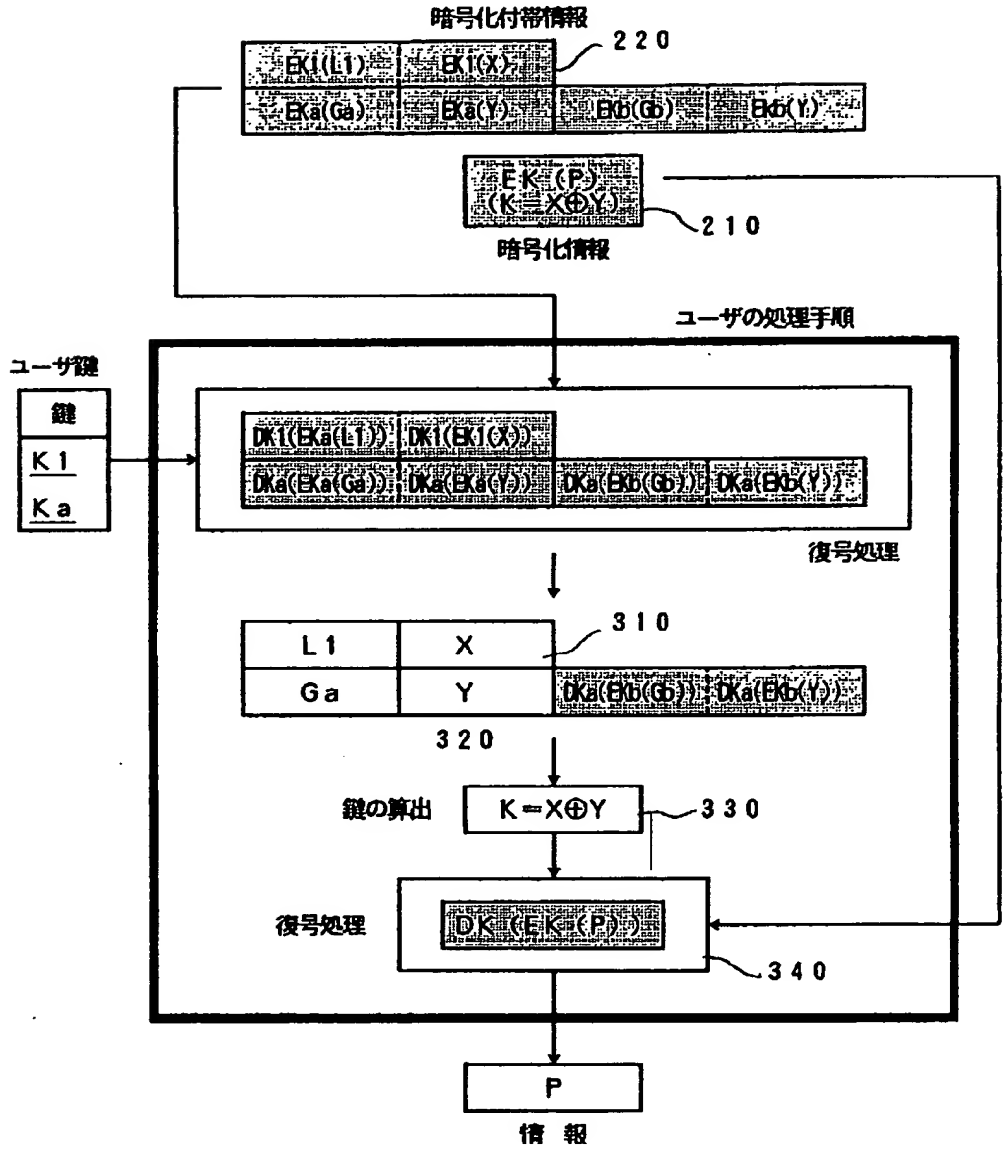
【図９】

情報共有システムに暗号化技術を適用した例を示す図



【図６】

本発明の第２の実施例のユーザが情報の参照を行う場合の処理を説明するための図



【図８】

共有システムの概要を示す図